I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV528707129US, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: August 17, 2004 Signature: (Sandy Reisman)

Docket No.: 324628004US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
C. Andrew Neff

Application No.:	09/534,836	Confirmation No.:	2620
Filed:	March 24, 2000	Art Unit:	3621
For:	METHOD, ARTICLE AND APPARATUS FOR REGISTERING REGISTRANTS, SUCH AS VOTER REGISTRANTS	Examiner:	Firmin Backer

APPELLANT'S BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This brief is in furtherance of the Notice of Appeal, filed in this case on June 22, 2004.

The fees required under 37 C.F.R. § 1.17(f) and 1.17(p) and any required petition for extension of time for filing this brief and fees therefor are dealt with in the accompanying FEE TRANSMITTAL.

This brief is transmitted in triplicate.

This brief contains items under the following headings as required by 37 C.F.R. § 1.192 and M.P.E.P. § 1206:

08/19/2004 HALI11 00000095 09534836
01 FC:2402 165.00 OP

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

VoteHere, Inc.

II. RELATED APPEALS AND INTERFERENCES

The applicant, the applicant's legal representative, and the real party in interest are unaware of any appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS[1]

A. Total Number of Claims in Application

There are 40 claims pending in the application.

B. Current Status of Claims

1. Claims canceled: None.
2. Claims withdrawn from consideration but not canceled: None.
3. Claims pending: 1-40.
4. Claims allowed: None.
5. Claims rejected: 1-40.

C. Claims On Appeal

The claims on appeal are claims 1-40.

In the first and final Office Actions, mailed June 12, 2003 and February 25, 2004, respectively, the Examiner stated that claims 1-40 were rejected under 35 U.S.C. § 102(e)

[1] Independent claims 1, 11, and 13 on appeal are quite similar to issued claims 1, 24, and 32, respectively, in European Patent No. 1224767.

as anticipated by a thesis by M. Herschberg, entitled "Secure Electronic Voting Over the World Wide Web." Attorneys for the applicant, however, believe that the rejection should be under 35 U.S.C. § 102(b), because the applied reference is not a U.S. patent or application.

IV. STATUS OF AMENDMENTS

The applicant has not filed any amendments after the last Office Action of February 25, 2004.

V. SUMMARY OF RELIED-UPON REFERENCE

Conventional voting schemes employ a two-step process. First, the voter registers, which typically includes the voter submitting his or her signature to a registrar. Second, the voter signs in at a poll, or signs an envelope enclosing a ballot, which allows the voter's signature to later be compared to the earlier-provided signature held by the registrar. Under the second step, systems are provided to keep the voter's identity confidential with respect to his or her ballot, and ensure that ballots are not compromised. *See, e.g.,* Application, page 2, lines 20-30.

Published articles and other references address how to provide electronic voting that ensures the privacy of each voter, as well as provide security to prevent voting fraud. Such references address ensuring the privacy of voters, such as through encryption, as well as authentication schemes to ensure that electronic ballots have not been tampered with. Such references, however, address only the second step in a voting process -- they fail to address registering voters.

The sole applied reference is a thesis by Mark Herschberg, entitled "Secure Electronic Voting Over the World Wide Web" (Massachusetts Institute of Technology,

1997).[2] Herschberg is directed to an electronic voting method conducted over the Internet, which employs known cryptographic processes, such as Blowfish (a block cipher) to encrypt communications, and standard public-private key generating software, such as RSA. Importantly, Herschberg, like the rest of the art, ignores how voters are registered. For example, at Section 6.4.2 entitled "Registration," Herschberg simply says the following:

> The Registrar can create ghosts. That is, it can register non-existent voters and later cast votes under those names. The prevention of ghosts is a policy issue, and not one for cryptography. A practical solution is to have adversarial parties oversee the registration process, to make sure the dead do not rise to vote again.

(Emphasis added.)

As can be seen from the above portion from Herschberg, Herschberg ignores registration as a cryptographic problem, and instead simply says that it is a policy decision. Similarly in Section 3.2.1 entitled "Authentication," Herschberg notes the following:

> The two options considered for vote identification are a public key system, suggested by the use of digital signatures in Fujioka et al., and a password system. The former was discarded for two reasons. . . . Second, either a public key system must already be in place, or the keys must be distributed in a secure manner. The most likely form of distribution would be for voters [to] get their keys during registration, which requires that they either remember the unwieldy number, or have some sort of secure electronic transfer available.

The above two sections in Herschberg appear to be the most relevant and the places where Herschberg would most likely discuss registration. However, neither of these sections addresses schemes for voter registration. Indeed, Herschberg simply ignores registration, and instead focuses on the process of handling encrypted ballots after registration (i.e., the second step in a voting process).

[2] A copy of the cited portions from the Herschberg reference is attached as Appendix B.

VI. SUMMARY OF INVENTION

The applicant's invention addresses voter registration, namely, the first step employed in conventional voting schemes. For example, one aspect of the invention describes a process of remote electronic registration 200, whereby a registrant submits a public key of a public/private key pair and identifying information to a registrar.[3] The registrar determines whether the registrant is eligible based on the provided identifying information. The registrar digitally signs public keys of eligible registrants and forwards the signed public keys to an authenticating authority for use in authenticating the source of encrypted voting information or electronic ballots submitted by registrants.[4] This first process is more convenient for the registrant than those below, but can be less secure. Claims 37-40 are generally directed to this aspect of the invention.

Under another aspect of the invention, a process of registration 300 employs a courier, such as a postal carrier, common carrier, or other means of hand-delivery. This process begins where the registrant produces a hash card including a printed copy of the hash of the public key of the registrant's public/private key pair as computed by the registrant.[5] The hash card may be any tangible medium capable of carrying the hash of the public key, as well as a physical, "live ink" signature of the registrant. Examples of such media include paper, destruction-resistant material (plastic or TYVEK™), and so forth.[6] The registrant physically signs and submits the hash card to a registrar via a

[3] Public key encryption equips a user with two keys, namely, a public key that a user may provide to everyone to encrypt messages for the user, and a private key, known only to the user, that is used to decrypt messages encrypted using the public key. Each public-private key pair is linked in a manner such that only the public key can be used to encrypt messages to a given recipient, and only the private key held by that recipient can be used to decrypt them. *See, e.g., Newton's Telecon Dictionary* 644 (19th ed. 2003).

[4] *See, e.g.*, Application, page 3, lines 2-8; page 10, line 26 – page 13, line 15; Figure 2.

[5] A "hash" generally refers to a value obtained through use of a hashing function. A hashing function is an algorithm that takes as input an original message or other input and produces a mathematical summary or value that ensures data integrity by detecting changes to the data caused by communication errors, tampering, and so forth. Hashing functions are typically one-way encryption schemes because the hash value can be readily computed based on the original message, but the original message cannot typically be determined based on the hash value. *See, e.g., Id.* at 375.

[6] *See, e.g.*, Application, page 13, line 30 – page 14, line 11.

communications channel such as a common courier. The registrant also submits his or her public key to the registrar electronically.

The registrar then independently computes the hash of the electronic public key as received. If the hash, as thus computed by the registrar, matches the hash printed on the received hash card, and the physical signature is deemed, by standard means, to match the physical signature of a legitimate voter, the registrar then digitally signs the public key. The registrar electronically forwards the digitally signed public key to an authenticating authority for use in authenticating the source of the encrypted voting information or electronic ballots submitted by the registrant.[7] This second process is generally more secure than that above, but can be less convenient for the registrant. Claims 1-20 are generally directed to this aspect of the invention.

Under a further aspect of the invention, a process of registration 400 employs a registrar 404 to produce public/private key pairs. This process begins where the registrar identifies a registrant 402 in-person, and provides the registrant with a private key of a public/private key pair in a secure manner, such as on removable media. The registrar digitally signs and forwards the public key to an authenticating authority for use in authenticating the source of encrypted voting information or electronic ballots submitted by the registrant, as noted above.[8] If the registrant 402 trusts the registrar 404, this third process provides more security than the above processes, but can be less convenient. Claims 35-36 are generally directed to this aspect of the invention.

Under yet another aspect of the invention, a process of registration 500 employs in-person identification and a registrant 502 generates a public/private key pair. This process begins where the registrant produces a hash card that that noted above, namely a card having a printed copy of the hash of the public key of the registrant's own generated public/private key pair. The registrant signs and submits the hash card to the registrar in-

[7] *See, e.g.*, Application, page 3, lines 9-16; page 13, line 20 – page 15, line 20; Figure 3.

person. The registrant also electronically submits the public key to a registrar. As noted above, the registrar verifies the registrant's submitted information and digitally signs the public key if the hash corresponds to the electronically submitted public key. Again, the registrar forwards the digitally signed public key to an authenticating authority for use in authenticating the source of encrypted voting information or electronic ballots submitted by the registrant.[9] This is the most secure of the above processes, but comes at the cost of convenience. Claims 21-34 are generally directed to this aspect of the invention.

In sum, the above registration processes describe how each eligible registrant obtains a public/private key pair that meets predefined format and security specifications of the registrar, authenticating authority, or both. A public key of each eligible registrant is distributed to or by an organization administering the registration (a registrar), and the registrar can digitally sign or otherwise maintain a record of each eligible registrant's public key. These inventive aspects protect the registrar from accepting and recording public keys from prospective registrants where the public keys have been generated by some illegitimate source, from nonexistent individuals, or are to be used for some illegitimate reasons. Thus, aspects of the invention are directed to registration processes so that the registrar can properly identify prospective registrants and record the public key of each prospective voter registrant.

VII. ISSUES

A. Has the Examiner failed to establish a prima facie case of anticipation because he has failed to explain what portions in Herschberg correspond to each of the claimed elements?

B. Does Herschberg fail to disclose any voter registration system for an electronic voting process?

[8] *See, e.g.*, Application, page 3, lines 17-21; page 15, line 29 – page 16, line 31; Figure 4.
[9] *See, e.g.*, Application, page 3, lines 22-29; page 17, line 7 – page 18, line 19; Figure 5.

C. Does Herschberg fail to disclose two different channels of communication, one of which includes hand-delivery, in a public key voter registration scheme?

D. Does Herschberg fail to disclose verifying voters/registrants in-person, or registration employing signatures on a hash card?

E. Does Herschberg fail to disclose in-person registration in an electronic voting scheme?

F. Does Herschberg fail to disclose digitally signing public keys by a registrar under an electronic voter registration method?

VIII. GROUPING OF CLAIMS[10]

For purposes of this brief only, and without conceding the teachings of any prior art reference, the claims have been grouped as indicated below:

Group I.	Claims 1-20 stand or fall together.
Group II.	Claims 21-34 stand or fall together.
Group III.	Claims 35-36 stand or fall together.
Group IV.	Claims 37-40 stand or fall together.

In Section IX below, the applicant has included arguments supporting the separate patentability of each claim group as required by M.P.E.P. § 1206.

IX. ARGUMENTS

A. The Examiner Has Failed to Establish a Prima Facie Case That Any of the Claims Are Anticipated Because He Has Failed to Explain What in Herschberg Corresponds to Each of the Claimed Elements.

The following is the entire rationale that the February 25, 2004 Office Action (the "Office Action") provides in rejecting claim 1:

[10] The applicant has grouped the claims to simplify issues on appeal. The applicant, however, does not admit that the claims in any group stand or fall together for purposes other than this appeal. In particular, the applicant reserves the right to argue the patentability of each claim separately in a subsequent action, such as reopened prosecution or litigation.

> As per claims 1, Herschberg teach a method of registration, comprising receiving a hash of a public key and a written signature of each of a plurality of registrants through a first channel of communications that includes hand-delivery, receiving a public key and associated identifying information of at least some of the plurality of registrants through a second channel of communications, different from the first channel of communications that excludes hand-delivery, for each of the plurality of registrants, digitally signing the public key if the hash of the public key of the registrant received through the first channel of communications corresponds to the public key of the registrant received through the second channel of communications; and providing the digitally signed public keys to an authenticating authority (*see abstract, Fig. 3.2, Chapter 3, 4*).[11]

As can be seen, the rejection simply copies claim 1 and provides a citation of Herschberg to two complete chapters spanning nearly forty pages. Similar rejections were provided for claims 2-10, namely, copying of these claims and citing to the same chapters of Herschberg. Regarding the remaining claims, the Office Action simply states "as per claims 11-40, they disclose the same inventive concept as in claims 1-10. Therefore, they are rejected under the same rationale."

As is known, to anticipate a claim under 35 U.S.C. §102, the reference must teach every element of the claim.[12] The Office Action fails to explain how each claim element corresponds to an identical element in Herschberg. Thus, a prima facie case for anticipation under 35 U.S.C. § 102(b) has not been met. If a prima facie case of anticipation has not been established, "then without more the applicant is entitled to grant of the patent."[13] The Office Action has not established a prima facie case of anticipation of claims 1-40, and for this reason alone, these claims are patentable.

[11] February 25, 2004, Office Action, pages 2-3.

[12] M.P.E.P. § 2131, at 70 (Feb. 2003, rev. 1). *See also Ex parte Levy,* 17 U.S.P.Q.2d 1461, 1462 (Bd. Pat. App. & Interf. 1990) (to establish a prima facie case of anticipation, the Examiner must identify where "each and every facet of the claimed invention is disclosed in the applied reference"); *Glaverbel Société Anonyme v. Northlake Mktg. & Supply, Inc.*, 45 F.3d 1550, 1554 (Fed. Cir. 1995) (anticipation requires that each claim element must be identical to a corresponding element in the applied reference); *Atlas Powder Co. v. E.I. duPont De Nemours*, 750 F.2d 1569, 1574 (1984) (the failure to mention "a claimed element (in) a prior art reference is enough to negate anticipation by that reference").

[13] *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

B. Herschberg Fails to Disclose Voter Registration Techniques in an Electronic Voting Scheme

As noted above, Herschberg is directed to employing cryptographic techniques in creating and casting a ballot. He ignores an important first part of any voting scheme, let alone an electronic voting scheme, namely, voter registration. Instead, Herschberg simply says that "the prevention of ghosts is a policy issue."[14]

Thus, Herschberg fails to disclose (or fairly suggest) any method of registration, which is the point of claims 1-40. Claims 1-10, 15-16, 21-28, and 34-40 are all directed to methods of registering voters or other "registrants." Claims 11-12, 17-18, and 29-32 are directed to computer-readable media whose contents cause a computer to register registrants, and claims 13-14, 19-20, and 33 are directed to computer systems for registering voters or registrants. Thus, claims 1-40 are patentable because Herschberg fails to disclose or fairly suggest a voter registration system for an electronic voting system.

The "Response to Arguments" section of the Office Action does explain the following:

> Herschberg teach the use of cryptographic techniques in creating and casting ballot. Herschberg does not fail to ignore registration of participant. Herschberg need not to address the registration of participant since it is inherent that in order for a party/(ies) to participate in Herschberg voting scheme, the party/(ies) must be a registered voter(s). It is well-known that non registered party/(ies) cannot participate in any voting process. Therefore, disclosing voting registration in Herschberg would be redundant.[15]

To the best of the applicant's understanding of this passage, the Office Action asserts that voter registration schemes are inherent or well-known in Herschberg.

Section 2112 of the Manual of Patent Examining Procedure (M.P.E.P.) explains that implicit and inherent disclosures of a prior art reference may be relied upon in rejecting

[14] As noted above, a "ghost" is a nonexistent voter.
[15] February 25, 2004 Office Action, page 5.

claims under 35 U.S.C. § 102. However, subsection IV of this section explains that the "Examiner must provide rationale or evidence tending to show inherency."[16] The M.P.E.P. goes on to explain that the "fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic."[17] To establish inherency, the extrinsic evidence in the reference must make clear (1) that the missing descriptive matter is necessarily present in the thing described in the reference and (2) that persons of ordinary skill would recognize that fact; inherency may not be established by probabilities or possibilities.[18]

The Office Action appears to argue that the entire point of the invention, namely, registration, is not disclosed in Herschberg, but need not be disclosed because it "would be redundant." This is improper. More to the point, the Office Action not only fails to make clear that the missing descriptive matter (registration) is necessarily present in Herschberg's system, but also fails to describe how it would be so recognized by persons of ordinary skill.

The Office Action does state that "[i]t is well-known that non registered [parties] cannot participate in any voting process." This is simply naïve. Recorded history in this country alone provides numerous colorful examples of voting fraud where dead people were registered so that their "votes" could be improperly included in an election. Voter registration is an important issue and, until now, not addressed in any electronic voting schemes of which the applicant is aware.

While not relevant to the asserted anticipation rejection, Herschberg does teach away from the claimed voter registration invention. Herschberg would instruct one of ordinary skill in the relevant art to ignore registration as a process unrelated to cryptography, and instead push it to public policy officials. The applicant disagrees. Registration instead is an element of voting that should be included in any electronic voting system, as now recited in the claimed invention. In conclusion, Herschberg not only fails to

[16] M.P.E.P., version 8, at 2100-54 (May 2004, rev. 2).
[17] *Id.* (citing *In re Rijckaert*, 9 F.3d 1531, 1534, 28 U.S.P.Q.2d 1955, 1957 (Fed. Cir. 1993)).
[18] *Id.*, (citing *In re Oelrich*, 666 F.2d 578, 581-82, 212 U.S.P.Q. 323, 326 (CCPA 1981)).

explicitly disclose registration, he fails to inherently disclose the claimed registration processes, and thus claims 1-40 are patentable over Herschberg.

C. Herschberg Fails to Disclose a Method of Registration that Employs Two Channels of Communication, One of Which Includes Hand-Delivery, in a Public Key Electronic Voting System.

Claim 1 recites that the method of registration includes "receiving a hash of a public key and a written signature of each of a plurality of registrants through a first channel of communications that includes hand-delivery." Further, claim 1 recites, among other limitations, "receiving a public key and associated identifying information of at least some of the plurality of registrants through a second channel of communications, different from the first channel of communications that excludes hand-delivery." As noted above, Herschberg fails to disclose any registration, let alone two different channels of communication for use in a registration process. The hash of the public key and written signature is provided via a hand-delivery channel of communications such as by common courier. Plainly, claim 1 is patentable over Herschberg.

The Office Action "Response to Arguments" section states:

> Applicant further argues that Herschberg failed to disclose two channels of communication that includes hand delivery. The channel of communication of the disclosed inventive concept indeed include hand delivery system, however, does not exclude electronic communication that is taught in Herschberg. It appears that a choice can be made to using either communication means in order for the delivery to be effective.[19]

To the best of the applicant's understanding of this statement, the Office Action attempts to argue that one of the two channels of communication can be electronic, and that Herschberg discloses electronic communication. However, this argument ignores the plain meaning of the claims. As noted above, claim 1 recites that the method of registration employs "a first channel of communications that includes hand-delivery," and "a second

[19] February 25, 2004 Office Action, pages 5-6.

channel of communications, different from the first channel of communications that excludes hand-delivery." Thus, claim 1 recites two channels of communication, one of which may be electronic, but the other of which is hand-delivery. Nowhere does Herschberg describe use of a hand-delivery channel of communications for voter registration. Again, claim 1 is patentable over Herschberg.

The remaining claims in Group I are patentable for similar reasons. Dependent claims 2-10 include all the limitations of independent claim 1, and are thus patentable for similar reasons. Claim 11 is similar to claim 1, but is directed to a computer-readable medium, while claim 12 is dependent on claim 11. Likewise, claim 13 is similar to claim 1, but is directed to a voter registration computer system, while claim 14 is dependent on claim 13. Independent claims 15, 17, and 19 include limitations similar to those described above with respect to claim 1, and are thus similarly patentable. Claims 16, 18, and 20 are dependent on claims 15, 17, and 19, respectively, and are thus similarly patentable. In sum, claims 1-20 are patentable because Herschberg at least fails to disclose (or fairly suggest) two channels of communication for voter registration, one of which includes hand-delivery, or a registration process of handling public keys via two channels of communication.

D. Herschberg Fails to Disclose Verifying Voters/Registrants In-Person, or Registration Employing Signatures on a Hash Card.

Claim 21 recites a registration method that includes "verifying an identity of [registrants] in-person." As noted above, Herschberg fails to disclose any registration of voters, let alone in-person registration. Thus, claim 21 is patentable over Herschberg.

Claim 21 goes on to recite "receiving a signature of the registrant on a respective hash including a written hash of the public key of the registrant." Nowhere does Herschberg disclose (or fairly suggest) use of a card or other tangible medium having a written or printed hash of a registrants' public key, let alone a written signature on that card. Again, claim 21 is patentable over Herschberg.

Remaining claims in Group II are patentable for similar reasons. Claims 22-28 are dependent on claim 21, and are thus patentable for similar reasons. Claim 29 is a computer-readable medium claim that recites limitations similar to those of claim 21, such as in-person verification of registrants and written signatures on a hash card containing a public key hash. Claims 30-32 are dependent on claim 29. Claim 33 is directed to a registration computer system, and again recites limitations substantially similar to those in claims 21 and 29, and is thus similarly patentable. Claim 34 is directed to a voter registration method, from the point of view of a voting authority that authenticates a number of public key encrypted votes. Importantly, claim 34 again recites similar limitations, namely, that registrants have their identities verified in-person and submit hash cards having a written signature and a printed hash of their public keys. Overall, claims 21-34 are patentable over Herschberg for at least the above reasons, namely, that Herschberg fails to disclose in-person registration and signatures on hash cards.

E. Herschberg Fails to Disclose In-Person Registration in an Electronic Voting Scheme.

As noted above, claims 35 and 36 are directed to a registration process employing a registrar to produce public/private key pairs for an electronic voting scheme, where the registrar identifies a registrant in-person. As noted above, Herschberg not only fails to disclose voter registration in an electronic voting scheme, but also fails to disclose in-person registration. Thus, claims 35 and 36 are patentable over Herschberg.

Claim 35 further recites "providing the private key of the respective produced public/private key pair to each of the registrants that have had their respective identities verified in-person." Herschberg fails to disclose this. For at least this additional reason, claim 35 is patentable over Herschberg.

F. Herschberg Fails to Disclose Digitally Signing Public Keys by a Registrar Under an Electronic Voter Registration Method.

As noted above, independent claims 37 and 40 of Group IV are directed to a remote electronic registration process for voters or registrants. As also noted above, Herschberg

fails to disclose (or fairly suggest) an electronic voter registration method. Possibly more importantly, and as recited in claim 37, one aspect of the invention employs "digitally signing . . . received public keys of the registrants." Claim 40 recites "receiving a plurality of digitally signed public keys from a registrar." Thus, claims 37 and 40 both recite that a registrar receives and digitally signs public keys associated with registrants or voters. Herschberg fails to disclose such. Thus, claims 37 and 40 are patentable over Herschberg. Further, claims 38 and 39 are dependent on claim 37, and are thus patentable for at least the same reasons.

X. CONCLUSION

The Office Action has failed to establish a prima facie case of anticipation of any of the claims. The Office Action simply restates the limitations of, for example, claim 1 and cites to chapters of Herschberg, without identifying where Herschberg even addresses aspects of the claimed invention, namely, voter registration. Further, Herschberg fails to not only address electronic voter registration, but also fails to disclose specific voter registration steps, such as: (1) registration employing two different channels of communication (one of which includes hand-delivery), (2) handling public keys via two different channels of communication, (3) verifying voters in-person for an electronic voting scheme, (4) employing signatures on a hash card, and (5) digitally signing public keys as part of an electronic voter registration process.

XI. CLAIMS INVOLVED IN THE APPEAL

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

The applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-0665, under Order No. 324628004US from which the undersigned is authorized to draw.

Dated: August 17, 2004

Respectfully submitted,

By _____

Christopher J. Daley-Watson
Registration No.: 34,807
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-3599
(206) 359-4599 (Fax)
Attorney for Applicant

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 09/534,836

1. A method of registration, comprising:

receiving a hash of a public key and a written signature of each of a plurality of registrants through a first channel of communications that includes hand-delivery;

receiving a public key and associated identifying information of at least some of the plurality of registrants through a second channel of communications, different from the first channel of communications that excludes hand-delivery;

for each of the plurality of registrants, digitally signing the public key if the hash of the public key of the registrant received through the first channel of communications corresponds to the public key of the registrant received through the second channel of communications; and

providing the digitally signed public keys to an authenticating authority.

2. The method of claim 1, further comprising:

rejecting the registrant if the hash of the public key of the registrant received through the first channel of communications does not correspond to the public key of the registrant received through the second channel of communications.

3. The method of claim 1 wherein receiving a hash of a public key and a written signature through a first channel of communications includes receiving a written message via a courier.

4. The method of claim 1 wherein receiving a public key and associated identifying information through a second channel of communications includes detecting a signal carried in at least one of an electrical, a magnetic, and an electro-magnetic carrier.

5. The method of claim 1 wherein the hash of the public key and the written signature of the registrants received through the first channel of communications are non-electronic.

6. The method of claim 1, further comprising:

providing each of the registrants a copy of the respective digitally signed public key.

7. The method of claim 1, further comprising:

creating a hash of the public key received through the second channel of communications for comparison to the hash of the public key received through the first channel of communications.

8. The method of claim 1, further comprising:

enabling the registrants to submit the public key and associated identifying information through the second channel of communications only after receiving the hash of the public key and written signature through the first channel of communications.

9. The method of claim 1, further comprising:

preventing the registrants from submitting the public key and associated identifying information through the second channel of communications

until after the hash of the public key and written signature are received through the first channel of communications.

10. The method of claim 1, further comprising:

entering the hash of the public key received though the first channel of communications into an electronic database.

11. A computer-readable medium whose contents cause a computer to register voter registrants by:

for each of a plurality of voter registrants, electronically receiving a hash of a public key that was transmitted by the registrant through a first channel of communications including hand-delivery;

for each of at least some of the plurality of voter registrants, electronically receiving a public key and associated identifying information that was transmitted by the voter registrant through a second channel of communications excluding hand-delivery;

for each of a number of the voter registrants, digitally signing the respective public key of the registrant if the hash of the public key received from the voter registrant corresponds to the public key received from the voter registrant; and

providing the digitally signed public keys to an authenticating authority.

12. The computer-readable medium of claim 11 whose contents further cause the computer to register voter registrants by:

creating a hash of the public key received through the second channel of communications for comparison to the hash of the public key received through the first channel of communications.

13. A voter registration computer system, comprising:

a public key hash input subsystem that for each of a plurality of voter registrants, electronically receives a hash of a public key that was transmitted by the voter registrant through a first channel of communications including hand-delivery;

a public key input subsystem that, for each of at least some of the plurality of voter registrants, electronically receives a public key and associated identifying information transmitted by the voter registrant through a second channel of communications excluding hand-delivery;

a digital signature subsystem that, for each of a number of the voter registrants, digitally signs the respective public key of the voter registrant if the hash of the public key received from the voter registrant corresponds to the public key received from the voter registrant; and

a digitally signed public key output subsystem that provides the digitally signed public keys to an authenticating authority.

14. The voter registration computer system of claim 13, further comprising:

a hashing subsystem that creates a hash of the public key received through the second channel of communications for comparison to the hash of the public key received through the first channel of communications.

15. A method of voter registration, comprising:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that submitted a hash of the public key through a first channel of communications including hand-delivery and that submitted the public

key corresponding to the hash through a second channel of communications excluding hand-delivery; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

16. The method of claim 15 wherein the public key encrypted votes are digitally signed by the respective voter registrants.

17. A computer-readable medium whose contents cause a computer to register voter registrants by:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that submitted a hash of the public key through a first channel of communications including hand-delivery and that submitted the public key corresponding to the hash through a second channel of communications excluding hand-delivery; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

18. The computer-readable medium of claim 17 wherein the public key encrypted votes are digitally signed by the respective voter registrants.

19. A voter registration computer system, comprising:

an input subsystem that receives a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that submitted a hash of the public

key through a first channel of communications including hand-delivery and that submitted the public key corresponding to the hash through a second channel of communications excluding hand-delivery; and

an authentication subsystem that authenticates a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

20. The voter registration computer system of claim 19 wherein the public key encrypted votes are digitally signed by the respective voter registrants.

21. A method of registration, comprising:

receiving a respective public key for each of a plurality of registrants;

for each of at least some of the plurality of registrants, verifying an identity of the registrant in-person;

for each of the verified registrants, receiving a signature of the registrant on a respective hash card including a written hash of the public key of the registrant;

for each of the verified registrants, digitally signing the public key received from the registrant if the hash on the hash card corresponds to the public key received from the registrant; and

providing the digitally signed public keys to an authenticating authority.

22. The method of claim 21, further comprising:

providing an acknowledged duplicate of the respective hash card to each of the verified registrants.

23. The method of claim 21, further comprising:

providing a copy of the respective digitally signed public key to each of the verified registrants.

24. The method of claim 21, further comprising:

rejecting the registrant if the hash on the hash card does not correspond to the public key received from the registrant.

25. The method of claim 21, further comprising:

providing a form for creating the hash card to at least some of the registrants.

26. The method of claim 21, further comprising:

providing a copy of public/private key pair generation software to at least some of the registrants.

27. The method of claim 21, further comprising:

prompting the registrants to generate the hash card; and

prompting the registrants to transmit the public key.

28. The method of claim 21 wherein identifying the registrant in-person includes at least one of comparing the registrant to a picture identification and comparing a signature of the registrant to a signature of the picture identification.

29. A computer-readable medium whose contents cause a computer to register registrants by:

receiving a respective public key for each of a plurality of registrants;

for each of at least some of the plurality of registrants, receiving an indication that an identity of the registrant has been verified in-person;

for at least a number of the verified registrants, digitally signing the public key received from the registrant if a public key hash submitted by the registrant on a hash card including a written signature of the registrant corresponds to the public key received from the registrant; and

providing the digitally signed public keys to an authenticating authority.

30. The computer-readable medium of claim 29 whose contents further cause the computer to register registrants, by:

automatically producing an acknowledged duplicate of the respective hash card for each of the verified registrants.

31. The computer-readable medium of claim 29 whose contents further cause the computer to register registrants, by:

rejecting the registrant if the hash on the hash card does not correspond to the public key received from the registrant.

32. The computer-readable medium of claim 29 whose contents further cause the computer to register registrants, by:

automatically providing a web page form for creating the hash card to at least some of the registrants.

33. A registration computer system, comprising:

a public key input subsystem that receives a respective public key for each of a plurality of registrants;

a tracking subsystem that, for each of at least some of the plurality of registrants, receives an indication that an identity of the registrant has been verified in-person;

a digital signature subsystem that, for at least a number of the registrants indicated as having identities verified in-person, digitally signs the public key received from the registrant if a public key hash submitted by the registrant on a hash card including a written signature of the registrant corresponds to the public key received from the registrant; and

a digital signed public key output subsystem that provides the digitally signed public keys to an authenticating authority.

34. A method of voter registration, comprising:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that have had their identity verified in-person by the registrar and that have submitted a hash card to the registrar including a written signature and a public key hash corresponding a public key electronically submitted to the registrar by the registrant; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

35. A method of registration, comprising:

for each of a plurality of registrants, verifying an identity of the registrant in person;

for at least some of the plurality of registrants, producing a public/private key pair;

for each of a number of the voter registrants that have had their respective identities verified in person, digitally signing the public key of the respective produced public/private key pair;

providing the private key of the respective produced public/private key pair to each of the registrants that have had their respective identities verified in-person; and

providing the digitally signed public keys to an authenticating authority.

36. A method of registration, comprising:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that have had their respective identities verified by the registrar in-person; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

37. A method of registration, comprising:

electronically receiving a public key and associated identifying data from each of a plurality of registrants over at least one communications channel;

digitally signing each of the received public keys of the registrants whose identifying data is not the same as the identifying data of the other registrants; and

providing the digitally signed public keys to an authenticating authority.

38. The method of claim 37 wherein digitally signing each of the received public keys of the registrants whose identifying data is not the same as the identifying data of the other registrants includes comparing the identifying data of at

least one of the registrants to the identifying data of at least another one of the registrants.

39. The method of claim 37 wherein electronically receiving a public key and associated identifying data includes receiving at least one of a registrant name, a registrant address and a unique registrant identifier.

40. A method of voter registration, comprising:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants having different identifying data from the other voter registrants; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.